UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER OF PATENTS AND TRADEMARKS
Washington, D.C. 20231
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/493,031	01/28/2000	Gideon Samid	4427-002	1677

7590 04/23/2002

BLANK ROME COMISKY & MCCAULEY, LLP
THE FARRAGUT BUILDING, SUITE 1000
900 17TH STREET, N.W.
WASHINGTON, DC 20006

EXAMINER
SEAL, JAMES

ART UNIT	PAPER NUMBER
2131	

DATE MAILED: 04/23/2002

Please find below and/or attached an Office communication concerning this application or proceeding.

Office Action Summary	Application No. 09/493,031	Applicant(s) SAMID, GIDEON	
	Examiner James Seal	Art Unit 2131	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If the period for reply specified above is less than thirty (30) days, a reply within the statutory minimum of thirty (30) days will be considered timely.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133).
- Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *31 January 2002* .

2a)☐ This action is **FINAL**. 2b)☒ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *17-33* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *17-33* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☒ The specification is objected to by the Examiner.

10)☒ The drawing(s) filed on _____ is/are: a)☐ accepted or b)☒ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

11)☐ The proposed drawing correction filed on _____ is: a)☐ approved b)☐ disapproved by the Examiner.

If approved, corrected drawings are required in reply to this Office action.

12)☐ The oath or declaration is objected to by the Examiner.

Priority under 35 U.S.C. §§ 119 and 120

13)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____ .

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

14)☐ Acknowledgment is made of a claim for domestic priority under 35 U.S.C. § 119(e) (to a provisional application).

a) ☐ The translation of the foreign language provisional application has been received.

15)☐ Acknowledgment is made of a claim for domestic priority under 35 U.S.C. §§ 120 and/or 121.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☐ Information Disclosure Statement(s) (PTO-1449) Paper No(s) _____ .
4) ☐ Interview Summary (PTO-413) Paper No(s). _____ .
5) ☐ Notice of Informal Patent Application (PTO-152)
6) ☐ Other:

DETAILED ACTION

1. The request filed on 31 January 2002 for a RCE based on parent Application No. 09493031 is acceptable and an RCE has been established. An action on the RCE follows.

2. New title is acceptable and has been entered.

3. New abstract is acceptable and has been entered.

4. Amendment to the specification, page 11 line 17 has been entered.

5. Claims 1-5, 7-13, and 16 have been cancelled without prejudice or disclaimer.

6. Claims 17-33 are pending.

Drawings

7. This application has been filed with informal drawings which are acceptable for examination purposes only. Formal drawings will be required when the application is allowed.

Objection to Specification

8. The disclosure is objected to because of the following informalities:

9. Page 9 line 21 and 22, page 41 line 16, page 70 line 5, the notation <> is use to denote "not equal" and according to the applicant is well known in the art. Examiner notes that the standard notation for "not equal" is ≠ and would respectfully request the applicant to supply examples of standard English mathematical or cryptographic references which supports that <> is used to denote "not equal". Objection maintained. The use of "( )" is objected to page 21 first paragraph because the applicant uses it for

two mathematically distinct ways and therefore the notation is confusing. In the first line the applicant write

$$ed = 1 \pmod{(n)}$$

and defines (n) in line 5 to be "the number of numbers less than n, which are relatively prime to n". It should be pointed out that the notation (n) and concept corresponds in standard mathematical and cryptographic textbooks to the Euler Totient function which is written as φ (n). For example, the RSA paper and patent use

$ed \equiv 1 \bmod \varphi(n)$ and all other textbooks (Schneier, Applied Cryptography; Menezes et. al. Handbook of Applied Cryptology. The examiner is not objecting to the use of new notation provided properly defined, nor the mathematics $(b^e)^d \bmod n = b$, but to the use of the notation ( ) being used in *two* different ways in the same paragraph. What makes this more objectionable is that the applicant places the caveat "the number of numbers less than n, which are relatively prime to n" directly beneath $(b^e)^d \bmod n = b$ rather than $ed = 1 \pmod{(n)}$ which would further imply to the reader that $(b^e)^d \bmod n = b$ is to be taken in some non standard. Examiner recommends that applicant use either the standard notation φ (n), or pick another notation which eliminates the confusion of two different mathematical usages in the same paragraph. Objection maintained.

10. Page 89, line 9, "(1)a" should be written "(1) a" to be consistent with rest of specification.

The examiner has listed the above instances as examples of informalities, the applicant is responsible for proofing his application.

Claim Rejections - 35 USC § 112

The following is a quotation of the second paragraph of 35 U.S.C. 112:

> The specification shall conclude with one or more claims particularly pointing out and distinctly claiming the subject matter which the applicant regards as his invention.

Claim 21 is rejected under 35 U.S.C. 112, second paragraph, as being indefinite for failing to particularly point out and distinctly claim the subject matter which applicant regards as the invention. Claim 21 recites "a subset of *contiguous* vertices" but as the word contiguous means being in actual contact, touching, or connected throughout, and the word vertex refers to a point a subset of points which are touching would imply one point. For the purpose of prior art the examiner will contiguous to mean neighboring.

Claim Rejections - 35 USC § 102

11. The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that form the basis for the rejections under this section made in this Office action:

> A person shall be entitled to a patent unless –

12. Claims 17-23 are rejected under 35 U.S.C. 102(b) as being anticipated by Matias et. al. U.S. 4910772 A.

13. As per claim 17, the limitation of a method of encryption (see Matias, Column 2, lines 14 and 39) converting a plaintext into a first symbol set, for example, English letters to a data stream, is common to all common encryption and is called encoding. Matias first encodes the communication information (which may be video or standard communication data stream, that is, plaintext, Column 4, line 22-23) into digital sequence of addresses (Column 4, lines 52-53, Column 7, line 25), and thus meets the

limitation of converting plaintext into a first symbol set. Matias meets the second limitation of creating a set of vertices which is associated with the first symbol set by forming an grid with the location of each vertex (pixel) given an address, the vertices depending on the original (first) symbol set (Column 2, lines 15-16, Column 5, lines 46-51). Matias meets the third limitation of defining relationship for pairs of vertices in the set of vertices (Matias' vertex grid or grid graph, Column 5, lines 57-60) wherein the relationship are expressed by vectors as determine by a pair of vertices. Matias meets the fourth limitation which uses the vectors to identify a path composed of at least one vector (Column 5, lines 56-59) and hence a second symbol set (up U, down D, left L, or right R, Column 6, lines 65-66) which are then used to specify the path. Matias does not limit his grid or graphs to rectangular arrays (Column7, lines 10-13) or even two dimensional (Column 10, line 68). Claim 17 is rejected.

14. As per claim 18, the limitation that no two consecutive symbols in the first symbol set are the same is met by Matias in that every pixel has a unique address. Claim 18 rejected.

15. As per claim 19, the limitation that there are at least as many vertices as there are symbols in the first symbol set and that at least one vector is associated with a pair of vertex is met by Matias (Column 5, lines 46-51). Claim 19 is rejected.

16. As per claim 20, the limitation of defining a relationship for pairs of vertices such that no two vectors originate in the same vertex are being associated with the same symbols of the second symbol set is met by Matias (Column 2, line 46). Claim 20 is rejected.

17. As per claim 21, the limitation of creating a set of vertices, such that, the subset of neighboring vertices associated with a set of symbols of the first symbols relate to vertices corresponding to any other symbols from the first set by a vectors originating originating in the first set of vertices and terminating in at least one vertex in the corresponding set of vertices. Matias mets this limitation as the addresses in the symbol set are associated with some subset of vertices, then addresses outside this domain of addresses will correspond to a different set of vertices but the vector associated with a pair of vertices one inside the other outside this domains are associated with symbols within the corresponding address of the first symbol set (Column 5, lines 45-51, lines 57-59, Column 6, lines 5--9). Claim 21 is rejected.

18. As per claim 22, the limitation of informing a recipient of the sequence the symbols from the second symbol sets about the locations of the vertices (Matias' U, D, L, R) and a initial vertex (start) is disclosed by Matias (Figure 1 elements 10 and 18, Column 8, lines 58-60). Claim 22 is rejected.

19. As per claim 23, the limitation of generating different keys for different message using the same encoding is disclosed by Matias Column 7, lines 55. claim 23 is rejected.

20. Claims 17-23 are rejected under 35 U.S.C. 102(b) as being anticipated by Krishnamurthy Compouter Cryptographic Techniques for Processing and Storage of Confidential Information.

21. Krishnamurthy disclose a number of methods for transforming plaintext into a secure form which can be communicated over insure links such that the secure form

can be transformed back into the original plaintext, without any intervening party being able to perform such transformations. Krishnamurthy discloses a number of transformation techniques including base conversion, modular arithmetic (groups, rings and fields), logic (Boolean logic), matrix, topological, functional and hierarchical (see page 753). Krishnamurthy discloses (page 760) methods for creating ciphers using addressing of arrays (after encoding) such that the encoded symbols (the first symbol set) are associated with an address-relational path (map) which is carried in the form of a description of heads (vertex), links (vectors) and ends of list (a designated point in the array the second symbol set). Claims 17-23 are rejected.

22. Claims 17-23 rejected under 35 U.S.C. 102(b) as being anticipated by Backal U.S. 6219421 A.

23. Backal discloses a method of encryption in which the content of message is not sent is not sent in its original (encoded form a first symbol set) or any transformation thereof, rather the encrypted message consists of a stream of pointers (vectors) to locations (address) (the second symbol set) in an arbitrary large array (of vertices) which serves as a (Virtual) key and thus allowing a very large key, the plaintext tracing out a path in the array. Claims 17-23 are rejected.

Claim Rejections - 35 USC § 103

24. Claims 24-33 are rejected under 35 U.S.C. 103(a) as being unpatentable over Matias as applied to claims 17-23 above, and further in view of Gaines.

25. Claims 24-33, recite a cryptographic method creating cryptanalytic obstacles by generating cryptographic key, which are graphs, by expressing the plaintext by a series

of vertices, from which a series of vectors which are in tern expressed in terms of U, D, L, or R (Matias notation) for which each vertex has no more than four nearest neighborings, in which the obstacles are built through the expansion of plaintext into larger ciphertext, by replacing any symbol with a group of symbols are replacing consective symbols with the same single symbolsand replacing U, D, L or R by the two binary digits 00, 01, 10, 11 is disclosed by Matias (Column 2, lines 15-16, 46; column 4, lines 22-23, 52-53; column 5, lines 46-51, 57-60; column 7, lines 10-13, 25; column 8, 58-60; and column 10 lines 68) as detailed above with Gaines providing the way of cryptanalytic obstacles through homophonic nulls (e.g. pg 201), which expands the ciphertext which one of ordinary skill in the art would have combined with the method of Matias to make it more secure. The use of binary vectors 00, 01, 10, 11 to represent U, D, L, and R in a computer environment is well known in the art. Claims 24-33 are rejected.

26. Claims 24-33 rejected under 35 U.S.C. 103(a) as being unpatentable over Krishnamurthy and alternatively Backal as applied to claims 17-23 above, and further in view of Gaines.

27. It would have been obvious for those of ordinary skill in the art to have combined these teachings with those of Gaines provides the homophonic nulls, and hence the cryptanalytic obstacle, to further secure the above encryption scheme.

28. Claims 17-23 are rejected under 35 U.S.C. 103(a) as being unpatentable over George Bush et. al. U.S. 5245658 A, and further in view of British War Office, Manual of Cryptography.

29. As per claim 17-33 Bush disclose a Domain-based cryptosystem in which uses identical domains (a grid or lattice, see Figure 4 or 7) known only to the parties involved in the communication. No plaintext or modification thereof is ever sent over the communication links. Instead messages are sent between communicating parties locating specific points (a second symbol set) in the domain which comprise a symbol set (first symbol set) which results from encoding the original plaintext message (Bush, Abstract, Figure 7. Summary). The cipher has homophonic nulls (see Column 2, lines 40-44) and hence the cryptanalytic obstacle. In Bush's scheme a central computer to establish an initial address in both sender and receiver domains (Column 4, lines 20-40). Bush sends addresses and not a stream of vectors, however, one of ordinary skill in the art could modify Bush's coordinate stream to a vector stream by relying on the line cipher taught by the Manual of cryptography, used by the British General Staff, War Office page 93 and 94. This would be more useful in the hardware of certain cipher system as it would require less memory.

30. Rejection of claims 17-33 under 103 Nakamura in view of Gaines is maintained.

Response to Arguments

31. Applicant's arguments filed 31 January 2002 and in interview with applicant and his attorney on 12 February 2002 have been fully considered but they are not persuasive.

32. With regards to the applicant's assertion that Nakamura differs from his applicantion in that his invention is a stream cipher and Nakamura is a block cipher, the applicant does not claim a stream cipher.

33. With regards to the applicant's assertion that Nakamura does not teach creating a set of vertices and defining (vectorial) relationship between pairs of vertices the examiner disagrees. The set of vertices and edges (links) used to define a graph (for example, figure 1) $G_n = (V, E)$ is indeed used to define associated link vectors $\mathbf{h}_i$ as defined by equation (2) and (3) where the $\mathbf{h}_i$ constitutes a row vector of the matrix h_{ij} and forms a linear basis of the graph space. Note that in the formula (2) that a link e_i always joins a pair of vertices.

34. With regards to the applicant's assertion that Nakamura by "creating a set of vertices" and by "defining a relationship for pairs of vertices in the set of vertices" is address (33) and using this to create an encryption key.

35. Nakamura associates the plaintext P to the character vector $\mathbf{Y}_0$ of G_n and the loop character vectors $\mathbf{Q}_i$ through the link vectors $\mathbf{h}_i$ through the matrix $\mathbb{H} = \{ \mathbf{h}_1, \mathbf{h}_2, \mathbf{h}_3, \ldots \mathbf{h}_m \}$ through equation (13)

$\mathbf{Q}_0 \equiv \mathbb{H}\mathbf{Y} \bmod M$. So $\mathbf{Q}_0$ is *related* to the vertex pairs of the graph through $\mathbb{H} = \{ \mathbf{h}_1, \mathbf{h}_2, \mathbf{h}_3, \ldots \mathbf{h}_m \}$. Then proceeding to page 43, Nakamura proves that all graphs $G_n(\mathbf{Y}_i)$ have the same loop-character vector $\mathbf{Q}_\theta$ and hence all graphs $G_n(\mathbf{Y}_i)$ are equavalent to the graph $G_n(\mathbf{Y}_0)$ through $\mathbf{Q}_\theta$ which is again defined through the vertex pairs V_i. This equivalence between the graphs is then interpreted as the process of encryption (converting plaintext to ciphertext) with the loop-character playing the roll of the key. As we have argued above, that the character is related to the plaintext graph then Nakamura's key is a vector derived from the graph and its vertex pairs. It should be further remarked that this equivalence along represents an "obstacle" to cryptanalyst as

pointed out by Nakamura (last line of page 43). However, if the "obstacle" referred to is more in accordance with what the applicant's discloses in the specification, then Gaines would have to be brought in if the applicant claimed such.

36. As to whether Nakamura is a "number theoretic" cipher (a point brought up in the interview with the applicant) as the applicant does not claim his approach as a non "number theoretic" cipher, this point would be moot. However I would point out that the Nakamura himself references books on graph theory (see references 3 and 4) and not number theory.

References Not Applied

37. With regards to the above discussion on notation, particular in regards to the Euler totient $\varphi(n)$ and his discussion of RSA, the examiner would like to offer the following references to support his claims:

a. Meneze et. al. Handbook of applied Cryptography, page 286

b. Simmons, Contemporary Cryptology, The Science of Information Integrity, page28, equation 42

c. Denning, Cryptography and Data Security, page 102 equation 2.4

e. Delf et. al. Introduction to Cryptography, Principle and Application page 31 equation 3.

d. Rivest, Shamir, and Adleman, A Method for Obtaining Digital Signatures and Public Key Cryptosystem page123 equation 5

Conclusion

38. Any inquiry concerning this communication or earlier communications from the examiner should be directed to James Seal whose telephone number is 703 308 4562. The examiner can normally be reached on M-F, 8-5.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Gail Hayes can be reached on 703 305 9711. The fax phone numbers for the organization where this application or proceeding is assigned are 703 746 7239 for regular communications and 703 746 7240 for After Final communications.

Any inquiry of a general nature or relating to the status of this application or proceeding should be directed to the receptionist whose telephone number is 703 308 3900.

JWS

Jws
April 19, 2002

GAIL HAYES
SUPERVISORY PATENT EXAMINER
TECHNOLOGY CENTER 2100